

# Reimagine Access Security for End-to-End Identity Protection

Using Layered Access and Privilege Controls to Prevent  
Modern Identity-Based Attacks

---

## Table of Contents

<b>The Epicenter of Modern Cyberattacks</b> .....	3
The Uncontrolled Privilege Gap .....	3
The Failure of Fragmented Tools .....	3
<b>Discover, Control, Govern with Idira Identity Security</b> .....	3
<b>Securing the Modern Workforce</b> .....	3
<b>Four Ways to Strengthen Workforce Identity Security</b> .....	4
1. Secure Identities Starting at the Endpoint .....	4
2. Secure Application and System Access at Login .....	5
3. Secure Access Beyond the Login for Added Protection .....	5
4. Govern Workforce Identities Across the Lifecycle .....	5
<b>Workforce Identity Security</b> .....	6
<b>Safeguard Your Future with Idira Identity Security Platform</b> .....	7
<b>About Palo Alto Networks</b> .....	7

---

## The Epicenter of Modern Cyberattacks

The threat landscape has fundamentally shifted. Today, identity weaknesses play a role in 89% of incident response investigations, and identity-based techniques drive 65% of initial access.<sup>1</sup> Attackers no longer break in. They log in, exploiting compromised credentials, bypassing basic authentication, and hijacking active sessions to blend in with normal activity.

### The Uncontrolled Privilege Gap

In the modern enterprise, the assumption that privilege is reserved only for IT administrators is obsolete. Rapid adoption of the cloud, SaaS, and automation means that every human identity holds immense privilege based on the sensitive targets they can reach and the actions they can take. This reality has created a massive uncontrolled privilege gap, where enterprise-grade security is applied to a small group of admins, while the rest of the workforce remains exposed.

### The Failure of Fragmented Tools

Traditional identity and access management (IAM) systems, like basic multifactor authentication (MFA) and single sign-on (SSO), remain foundational. As a single checkpoint at login, however, they cannot fully defend against today's advanced attacks. Historically, organizations have fragmented identity security into disconnected disciplines: IAM for the front door, privileged access management (PAM) for IT admins, and identity governance and administration (IGA) for compliance. Because attackers don't respect these category boundaries, they exploit the dangerous gaps left between these siloed tools.

## Discover, Control, Govern with Idira Identity Security

To close the uncontrolled privilege gap, organizations must shift from fragmented tools to a unified identity security operating model. Idira™ Identity Security Platform, by Palo Alto Networks, is the industry's first AI-native platform that converges IAM, PAM, and IGA into a single operating model for every human identity.

The Idira framework is built on three critical pillars:

- **Discover:** Continuous, automated discovery of every human identity, account, and entitlement across on-premises, cloud, and SaaS environments to build a live inventory of privilege before attackers find it.
- **Control:** Enforcing layered, adaptive controls from the endpoint to any target, ensuring that every human identity operates with least privilege by default, dynamically adapting to real-time risk.
- **Govern:** Automating lifecycle management to ensure access continuously aligns with business needs, behavior, and risk, from the moment an identity is created to its final departure.

This whitepaper focuses on the Control pillar of the Idira framework.

## Securing the Modern Workforce

Securing today's dynamic, distributed workforce is no easy task, considering it's made up of workers ranging from employees, contractors, and freelancers to partners, application administrators, and vendors. They can work from any location—home, the office, or the road—using any company-supplied or personal device. And, they access an array of applications, such as cloud-native business apps, conventional on-premises applications, and SaaS solutions.

---

1. *Unit 42 Global Incident Response Report 2026*, Palo Alto Networks, February 17, 2026.

Every worker, regardless of their role, can be a privileged, high-risk user. Also, any user can become a potential target based on their rights, access to sensitive data, and role in critical workflows. To secure the workforce, organizations must protect every user's identity, manage their privileges, and monitor and control their actions. It starts with securing their endpoints.

Now, more than ever, organizations must safeguard users' credentials, browsers, and machines they work on, closely governing their evolving permissions from their first day to their last day on the job.

## Four Ways to Strengthen Workforce Identity Security

Organizations can defend against modern identity-based attacks by introducing layered access and privilege controls across the entire user journey and employee lifecycle. An end-to-end approach safeguards every user interaction, from login and beyond, providing continuous protection against preauthentication and postauthentication attacks. It manages workers' fluctuating roles and privileges throughout their tenure, improving governance and oversight.

Figure 1 illustrates four ways Idira strengthens workforce identity security, defends against modern attacks, and mitigates risk. The following sections explain each approach.



Figure 1. Four ways to strengthen workforce identity security

### 1. Secure Identities Starting at the Endpoint

The user journey begins at the endpoint. Whether it's a workstation or a server, each endpoint includes built-in administrative accounts. If the endpoints contain vulnerabilities, configuration errors, or standing permissions, adversaries can exploit them by gaining access to privileged accounts, moving laterally, and orchestrating attacks. Costly supply chain attacks and ransomware attacks targeting endpoints are commonplace.

To prevent such attacks, use an endpoint privilege manager solution, like Idira Identity Security Platform, to control access and privilege at the endpoint. Continuously discover and remove local admin rights from workstations and servers and provide just-in-time (JIT) privilege elevation and fine-grained application controls to enforce the principle of least privilege and limit exposure. Monitor and detect unauthorized access to passwords, credentials, hashes, cookies, and other security tokens, improving visibility into suspicious activity symptomatic of an identity-driven attack.

By hardening endpoints and reducing the attack surface, endpoint identity security solutions help defend against zero-day attacks, contain lateral movement and ransomware spread, and mitigate insider and external threats. They also help support zero trust security frameworks and provide evidence of compliance and readiness for auditors and cyber insurance underwriters.

---

## 2. Secure Application and System Access at Login

Use an IAM solution to authenticate users and control access to critical applications and services at login. Implement SSO to eliminate credential sprawl and reduce your attack surface. SSO gives workers secure access to all applications and systems by using a single set of credentials—reducing exposure while improving user experience.

Implement adaptive MFA to ensure each user is who they say they are. Choose phishing-resistant authentication factors, such as smart cards, passkeys, and biometrics, that best meet your security and usability needs. Use contextual information, such as user risk, location, device, and time of day, to determine which authentication factors to apply to a specific user in a particular situation. Adaptive MFA strengthens security without encumbering users.

Use a password manager to enhance the security of nonfederated apps. Password managers reduce vulnerabilities by removing passwords from endpoints and browsers. They also eliminate password fatigue and risky workarounds like workers reusing passwords or tracking them on paper or in plain-text files. Because credential theft is a major concern, securely store all credentials in a centralized digital vault for ultimate protection, control, and administrative simplicity.

## 3. Secure Access Beyond the Login for Added Protection

While securing access at login is fundamentally important, it's insufficient. Threat actors can hijack active sessions and exploit privileged identities to exfiltrate data or carry out attacks. To prevent such events from happening, implement both step-up authentication and continuous authentication. These added protections secure high-risk users beyond the initial login and safeguard against advanced identity-driven attacks.

Use *step-up authentication* to revalidate users before they perform high-risk actions like installing software or running applications with elevated privileges. Step-up authentication is crucial for enhancing security, while maintaining usability. It ensures users can perform low-risk actions with minimal friction, but it requires additional verification for operations that might be employed in an attack. Step-up authentication helps protect against cookie theft and other types of session abuse and malicious incidents.

Use *continuous authentication* to revalidate high-risk users after a predefined period of time or inactivity. Continuous authentication protects against session hijacking and unauthorized application access and defends against adversary-in-the-middle (AitM) or meddler-in-the-middle (MitM) attacks. Leading identity security platforms can automatically reauthenticate users if they engage in unusual behavior.

Deploy secure browsers to safeguard access to web apps, SaaS solutions, and cloud consoles. You can use a secure browser to block access to unsanctioned URLs, suppress clipboard functionality, prevent file transfers, and restrict browser extensions. Secure browsers help combat malware and data exfiltration, as well as mitigate cookie theft and browser-in-the-middle attacks.

## 4. Govern Workforce Identities Across the Lifecycle

Managing user identities and access rights is a challenge for many information security organizations. Many rely on manually intensive, disjointed processes to onboard users and manage their evolving privileges. This time-consuming and error-prone approach hinders IT service agility, squanders resources, and is fraught with risk. It can take days or weeks to grant new hires secure access to the tools they need to perform their jobs. Also, tracking and reassigning user privileges across disparate applications and systems as people change roles is just as complicated. Threat actors can exploit misprovisioned, overprivileged, or orphaned accounts to launch attacks or steal data.

Use an identity lifecycle management solution, like Idira Identity Security Platform, to automatically onboard workers and manage their permissions throughout their tenure. Identity lifecycle management tools automate routine provisioning tasks, making it easy to add accounts and manage privileges as workers change roles and responsibilities. Most identity lifecycle management solutions support a wide variety of enterprise applications and services. Many integrate with HR and human capital management (HCM) systems to automate new-hire onboarding. They can also include self-service capabilities and automated workflows to streamline permission requests and approval processes and simplify change management.

Lifecycle management solutions improve IT productivity by eliminating manual processes. They also reduce security vulnerabilities by eliminating overpermissioned and dormant accounts that internal or external threat actors can exploit.

## Workforce Identity Security

Defending against modern identity-based attacks requires layered access and privilege controls across the entire user journey. From securing identities at the endpoint and fortifying the initial login, to protecting active sessions and automating the identity lifecycle, each control plays a vital role in preventing preauthentication and postauthentication attacks.

Acquiring these capabilities through disconnected point solutions is no longer a viable strategy. Treating IAM, PAM, and IGA as separate disciplines creates a structural liability. If these controls operate in silos, an attacker can bypass the IAM front door and exploit standing access that PAM has never seen and IGA hasn't reviewed.

Workforce identity security is designed to secure every worker's identity throughout their digital journey with the right level of access and privilege controls across all environments. Idira Identity Security Platform sets a new foundation for identity security to defend organizations against preauthentication and postauthentication identity-based threats by layering MFA, SSO, and lifecycle automation with endpoint identity security, browser security, password protection, and web session security. The solution set includes advanced AI features and proven threat detection and response capabilities to ensure the digital journeys that users take daily do not become attack pathways.

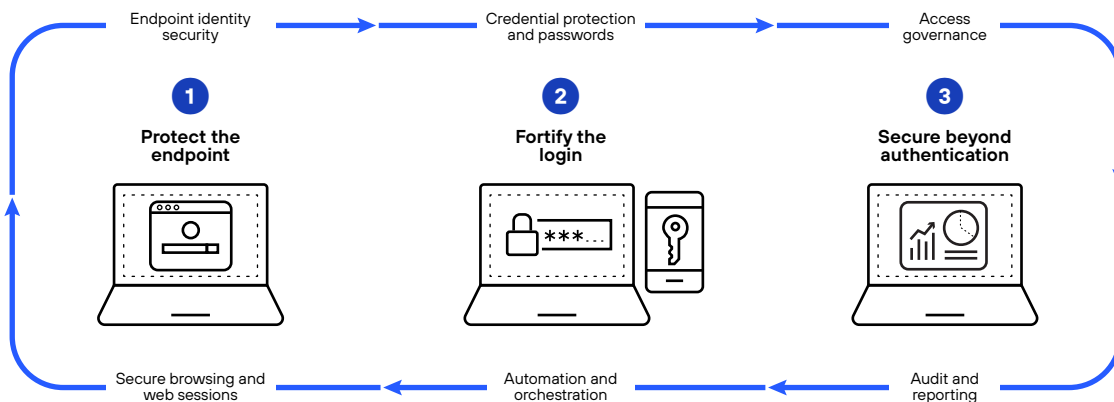


Figure 2. End-to-end workforce identity protection

---

## Safeguard Your Future with Idira Identity Security Platform

The future of securing your workforce lies in platformization. Idira Identity Security Platform converges IAM, PAM, and IGA, giving you one data model, one policy engine, and one governance layer. In this unified model, Discovery informs Control, Control informs Governance, and Governance continuously informs your overall risk posture.

By using the Idira framework, your organization applies enterprise-grade privilege controls to every human identity, not just the IT admins. This holistic approach enables your organization to reduce operational and security risks, satisfy audit and compliance requirements, and empower all users to securely access any resource, from anywhere, without friction.

Idira Identity Security Platform, which is built on the idea of securing every identity with the right privilege control levels, employs a reimagined approach to workforce access to:

- Deliver measurable cyber risk reduction.
- Drive operational efficiencies.
- Enable digital transformation.
- Satisfy audit and compliance.

To explore all the ways Idira can secure the identities across your organization, visit [\[link TK\]](#).

## About Palo Alto Networks

Palo Alto Networks (NASDAQ: PANW), the global AI cybersecurity leader, protects our digital way of life with a comprehensive portfolio of cybersecurity solutions and platforms across Network, Cloud, Security Operations, AI, and Identity. Trusted by more than 70,000 customers and powered by Unit 42® threat intelligence, our AI-driven platforms eliminate complexity, empowering enterprises to modernize with confidence and securing the speed of innovation. Explore the future of security at [www.paloaltonetworks.com](http://www.paloaltonetworks.com).



3000 Tannery Way  
Santa Clara, CA 95054  
Main: +1.408.753.4000  
Sales: +1.866.320.4788  
Support: +1.866.898.9087  
[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.

idira\_wp\_reimagine-access-security-for-end-to-end-identity-protection\_040926